Standard Operating Procedure (SOP)

ČNRDD/M02/verze 01

Electronic Records

1. Goal

The Coordination Centre uses a computer database system for data processing and storage. Everyday CC activity is based on electronic records. The Coordination Centre uses the information system of BMDR (programme), EMDIS and BMDRLAB.

2. Scope of Application

CC operator
Database Administrator   Programmer

3. Competences and Responsibilities

3.1. CC operator: starts and ends the programme, makes and edits entries, creates printouts and forms, prints printouts, has the authorisation to modify code lists of the programme, communicates with the programmer.
3.2. Database Administrator: regularly backs up the database and solves potential problems of the central database on the server, loads new programme versions.
3.3. System Administrator: solves potential faults at the workstation (PC) or operating system (OS), solves faults in the access to CIS, the internet and e-mail, he/she does not have access to the programme and BMDR database.
3.4. Programmer: creates and modifies the programme, issues new versions of the programme, is entitled to intervene with the programme and the database.

4. Abbreviations and Definitions

4.1. BMDR: Bone Marrow Donor Registry – the name of the programme
4.2. EMDIS:
4.3. CC: Coordination Centre
4.4. SW   Software
4.5. UWB   University of West Bohemia

5. BMDR Programme

5.1. Programme description

5.1.1. The author of the information system SW of CC – BMDR programme – is the University of West Bohemia, the Department of Applied Sciences. The system was put into operation in 2002.
5.1.2. The author and contractor of SW for EMDIS is the University of West Bohemia, the Department of Applied Sciences. The programme was put into trial operation in November 2008.
5.1.3. Data are stored at the SQL database on the server. The used Interbase database works on the transaction principle, i.e. every process commenced in the database is

| Processed by: MUDr. Helena Pittrová date: | Verified by: MUDr.Kateřina Steinerová date: | Approved by: MUDr.Vladimír Koza date: |

marked as a start of the transaction and the entry to the database only occurs after its successful completion. Therefore, the data are always consistent, even in a physical failure of the server.

5.1.4. The system is installed on the UWB server. Individual workstations (3 in total) from which it is possible to access the system are situated in CC.

5.1.5. The regular hardware and operation system maintenance is ensured by the UWB System Administrator.

5.1.6. The programme consists of several mutually related and interconnected modules. There are 5 main modules: a) Donors, b) Donors – Foreigners, c) Candidates, d) Archives and e) Service.

5.1.7. The system also includes lists and code lists containing supportive data for the system operation and control. Special modules providing some special functions such as donor selections according to the given criteria, statistic printouts, etc. are also available.

5.2. Programme versions and modifications

5.2.1. The author of the system (programmer) distributes innovated versions of the programme by means of an encoded attachment to an e-mail or through a flash disk. The contractor sends a notification of the new version to the Database Administrator who ensures the programme update and enters the new version into the *BMDR Programme Operation Logbook.*

5.2.2. The contractor of the system shall perform validation before distributing the new version which shall verify existing consistency and functionality of the system compared to the previous version.

5.2.3. The programmer shall send the *BMDR System Revision Protocol* to the Chief CC Operator. The operator shall sign the protocol and put it in the *BMDR* folder.

5.2.4. The CC operator must familiarize the other workers with significant changes in the system affecting the ordinary operation or he/she shall incorporate the change to the standard operating procedures.

5.2.5. The current version number is available in the Service menu, where changes made in the system can be found with the respective date.

5.3. Access rights and security

5.3.1. Every operator has his/her unique user (log-in) name and password necessary for the programme start-up.

5.3.2. After finishing or suspension of the work with the database (even during a day) the workers shall always end the programme. To open the system again, they must log in. The worker must not work with the programme when logged in under a different than his/her own! It is necessary to log in, in the event of a change of the user.

5.3.3. The system automatically records the work history, therefore it is possible to identify both the worker and the exact date, when he/she had worked with the programme (or was logged in to the system).

5.3.4. The programmer and the Database Administrator have the highest level of access authorisation 5. At this level it is possible to update the programme, add or remove users and change their authorisation level.

5.3.5. The CC operator with authorisation 4 can add or remove users in the database administration and change their level of authorisation.

5.3.6. All workers of the Coordination Centre have a basic access password (authorisation level 3). The Chief CC Operator has an administrator password (level 4) which enables him/her to make some changes in the system setting or correct errors which occurred during work with the database.

Processed by: MUDr. Helena Pittrová date:	Verified by: MUDr.Kateřina Steinerová date:	Approved by: MUDr.Vladimír Koza date:

5.4. Training of workers

5.4.1. Every new worker must be trained in using the BMDR programme within initial training.

5.4.2. He/she can work independently with the system and make records only after complete training and after this competence has been granted by the CC Manager in writing. Only then an access password is attributed.

5.4.3. After issuing a new version or a more significant modification all workers must be familiarized with the changes within regular CC personnel trainings. The Chief CC Operator is responsible for the training.

5.5. Data integrity validation and testing

5.5.1. Data integrity is validated and tested once a year (the system supplier) at the end of a calendar year.

5.5.2. A group of 5 tested donors and 5 tested candidates is created. The completeness and formal correctness of items and data records associated with entering the donor data and search for the tested candidates are checked on them.

5.5.3. A group of real donors and candidates is also used, on which the data stored in the database are verified and the agreement of the displayed data with their printed form is then verified (CC record documentation).

5.5.4. The result of such validation is an *Annual Validation Protocol* which is handed over to the Chief CC Operator by the supplier. He/she shall confirm acceptance and familiarisation with the protocol.

5.5.5. A precise procedure of validation is described in "BMDR – Operation Control Programme".

5.6. Database maintenance

5.6.1. An Information System Administration (ISA) worker is responsible for routine maintenance; the Database Administrator is responsible for the BMDR system.

5.6.2. In the event of any instability, atypical behaviour or functional failure of the database the respective worker shall inform the CC operator and vice versa.

5.6.3. The CC operator shall determine character of the fault and shall try to find a solution together with the Database Administrator. If the fault is not removed, he/she shall contact the programmer (the programme supplier).

5.6.4. Potential failures of the system and significant upgrades are recorded in forms *Controls: BMDR Program (SOP...)* or *Failures: BMDR Programme (SOP).* The Chief CC Operator is responsible for this.

5.7. Record uniqueness preservation

5.7.1. Within the BMDR programme not only the uniqueness of individual records must be preserved, but also the uniqueness of donor and patient IDs.

5.7.2. The system automatically checks the uniqueness of donor ID, names and Birth ID No. of candidates to eliminate duplicities.

5.8. OS and PC inspection

5.8.1. ISA ensures regular inspections of the operating system and the client PC hardware. ISA is also responsible for the functioning of the server, where the central database is situated. ISA performs central updates of OS and the security software.

Processed by: MUDr. Helena Pittrová date:	Verified by: MUDr.Kateřina Steinerová date:	Approved by: MUDr.Vladimír Koza date:

Valid from: Page: 3/8

5.8.2. Potential hardware faults shall be announced by the CC operator to the ISA operator (helpdesk) who will ensure removal of the fault by distant access or a service intervention of an ISA worker directly in situ.

5.8.3. The client PC (and the whole computer network of the Faculty Hospital) is protected by an antivirus programme administered by ISA with no interventions of the CC workers. Anti-spy software is started by a CC worker on the client PC in regular intervals (once a week).

5.9. Troubleshooting

5.9.1. Any problem is first solved with ISA workers or by phone with the workers of the Balák /Fatka Company.

5.9.2. In the event of accident the system supplier shall ensure recovery of the programme operation (if needed by using the latest backup) and data rescue.

5.10. Procedure in case of accident

5.10.1. Power supply failure
    5.10.1.1. The system does not require any action; it is immediately functional upon the power supply renewal. For safety it is connected through USB.

5.10.2. Hardware failure
    5.10.2.1. If the programme reports that the database is unavailable, the failure is probably in the network or server. We inform the SIS worker.
    5.10.2.2. If the server is accessible from the workstation, a database failure probably occurred. The ISA worker shall contact the programme supplier and together they shall try to repair the programme. If the repair is unsuccessful, we proceed according to the following point.

5.10.3. Loss of database
    5.10.3.1. If the database is lost, it must be recovered from the backup upon putting the server into operation.
    5.10.3.2. The database is fully functional immediately after recovery. All lost data must be added to prevent the loss of the data informative value. This shall be ensured by the CC Coordinator.

6. Procedure

6.1. Work with the programme

6.1.1. The work with the BMDR programme is governed by the valid user manual. The manual is divided to several parts: a) General overview, b) Donors c) Donors - foreigners, d) Candidates e) Archive … etc. the manual is stored among the CC documentation.

6.1.2. A brief user manual available at CC serves for everyday orientation.

6.2. Record acquisition

6.2.1. A record is made in real time, i.e. <u>concurrently</u> with the performed steps we describe.

6.2.2. Various data are entered in the predefined fields (where we move according to the general principles for working with Windows tabulator, enter, arrow):
- Numeric values
- Text
- Selection from the list of the predefined items

| Processed by: MUDr. Helena Pittrová
date: | Verified by: MUDr.Kateřina Steinerová
date: | Approved by: MUDr.Vladimír Koza
date: |

Valid from: Page: 4/8

6.2.3. Before leaving the given page/folder of the programme the correctness of entered data must be checked.

6.3. Record verification

6.3.1. All data entered in the programme are checked by a worker making the record (operator) before their confirmation. Another check is performed after printing the data – a CC operator.

6.3.2. There is a predefined format for entering data to the programme fields which only allows for entering the information of the required type or the entry to the field is limited to a list of values set by the respective code list. After entering a new/faulty record a question about its verification appears.

6.3.3. Before some important steps (a record deletion, modification, etc.) the system asks the user before implementing the command.

6.4. Printouts

6.4.1. Most events entered in the BMDR programme are printed after the data completion and stored. This enables an independent data revision.

6.4.2. The list of all printouts from the programme (and modules, from where printing is carried out) is given in the table.

NUMBER	NAME	CONTENT
1	A1DNA	PRELIMINARY WITH HLA-DNA
2	F1	ACTIVATION FOR DC AND HOU LAB (Haematological - Oncological Unit Lab)
3	F2	DOCUMENT FOR INVOICING
4	F3	ACTIVATION RESULT
5	BG	LIST OF DONOR BG ACCORDING TO FORM F1
6	CT-DHL-EU	SENDING CT TO EU BY DHL
7	CT-DHL	SENDING CT OUTSIDE EU BY DHL
8	CT-FEDEX	SENDING CT TO EU BY FEDEX
9	CT-PLZEŇ	SENDING CT FROM PLZEŇ-HOU TO EU BY DHL
10	CT-PRAHA	SENDING CT FROM PRAHA-HOU TO EU BY DHL
11	CT-WC	SENDING CT TO EU BY WORLD COURIER
12	CT-REQ	REQUEST FOR CT
13	CT-ARR	BLOOD COLLECTION FOR CT ANNOUNCEMENT
14	CT-RES	CT RESULT
15	CT-WORD	EXTRACT OF THE CT RESULT FROM LAB TO WORD
16	IDM-REQ	REQUEST TO DC FOR COLLECTING A SAMPLE TO IDM
17	IDM-RESULT	IDM RESULT
18	CT-DC	REPORT FOR DC ON THE CT RESULT
19	CT-E RES	REQUEST FOR SENDING THE CT RESULT IN ENGLISH
20	CT-C RES	REQUEST FOR SENDING THE CT RESULT IN CZECH
21	ES-ČEK	END OF SEARCH DR, CT
22	ES-TX	END OF SEARCH BY COLLECTION
23	UNAV	DONOR´S DISABILITY
24	CANC	SEARCH CANCELLATION
25	WU-BM	INFORMATION FOR TC ABOUT BM HARVEST
26	WU-BMCS	INFORMATION FOR TC ABOUT BM HARVEST

Processed by: MUDr. Helena Pittrová date:	Verified by: MUDr.Kateřina Steinerová date:	Approved by: MUDr.Vladimír Koza date:

Valid from: Page: 5/8

27	WU-KB	INFORMATION FOR TC ABOUT HSC COLLECTION
28	WU-KBCS	INFORMATION FOR TC ABOUT HSC COLLECTION
29	MONITORING	LETTER TO THE ==PRACTITIONER==

6.5. Database backup

6.1.1. The database is backed up automatically on a daily basis (compressed backed up data are gradually saved in cycles in the range of 7 days) at night both on the database server on the local disk at 0:15 a.m. and on the local disk R of the administrator server at 0:05 a.m.

6.5.1. Another backup is mirror disks of the UNIS server, where the same data are concurrently recorded and in the event of damage to one disk the data can be obtained from the other. A special source (UPS) is available to prevent damage of the data during power failure which ensures power supply to the server for the period of approximately 5 minutes.

6.5.2. Data archiving: If needed (approximately once a week) the compressed databases of the BMDR application are archived to a flash disk and the backup server R of the Information System Administration of the Faculty Hospital. An operator and the SIS worker administrating the BMDR system are responsible for archiving. The backup creation is recorded in the *BMDR Programme Operation Logbook.*

6.6. Procedure during a programme failure

6.6.1. When the programme fails, the continuing operation of the Coordination Centre must be ensured until the problem is removed.

6.6.2. If a non-standard behaviour of the programme occurs or it is not functional, the operator shall proceed according to Item 5.9.

6.6.3. For the period of the system failure availability of records is ensured as follows:
- All older records are printed and stored in the Coordination Centre,
- New records are entered to pre-printed forms.

6.6.4. After the system commencement all data are retrospectively entered in a standard way. The CC operator is responsible for this task.

7. Quality Control

7.1. Locking of records

7.1.1. Records in the BMDR programme are locked after some time (3 months?) and they are only available for reading. This ensures the uniqueness of records.

7.1.2. A change of the locked record can be initiated only by the CC operator. A change is made, after consulting with the programmer, by the programmer himself or the Database Administrator according to the programmer´s instructions.

Processed by: MUDr. Helena Pittrová date:	Verified by: MUDr.Kateřina Steinerová date:	Approved by: MUDr.Vladimír Koza date:

Valid from: Page: 6/8

7.1.3. Before making a change it shall be thoroughly considered, whether or not the intervention will lead to a disturbance of the database integrity and completeness. Due to this reason it is not allowed to completely delete records, but only to modify them.

8. EMDIS

9. Documentation

9.1. *The Annual Validation Protocol (*BMDR programme) is stored at CC (the Chief CC Operator is responsible).
9.2. *BMDR System Revision Protocol* is deposited in the BMDR folder.

10. Forms

10.1. BMDR Programme Operation Logbook
10.2. Data Backup Operation Logbook

11. Related SOP

12. Miscellaneous

NA

13. References

13.1. The BMDR Programme Manual (the Balák Company).

| Processed by: MUDr. Helena Pittrová
date: | Verified by: MUDr.Kateřina Steinerová
date: | Approved by: MUDr.Vladimír Koza
date: |

Valid from: Page: 7/8

CHANGES/REVISIONS:

Date:	Revised by/Approved by:	Signature:	Revision/Change*:

* Regular annual revisions marked bold.

Processed by: MUDr. Helena Pittrová date:	Verified by: MUDr.Kateřina Steinerová date:	Approved by: MUDr.Vladimír Koza date:

Valid from: Page: 8/8